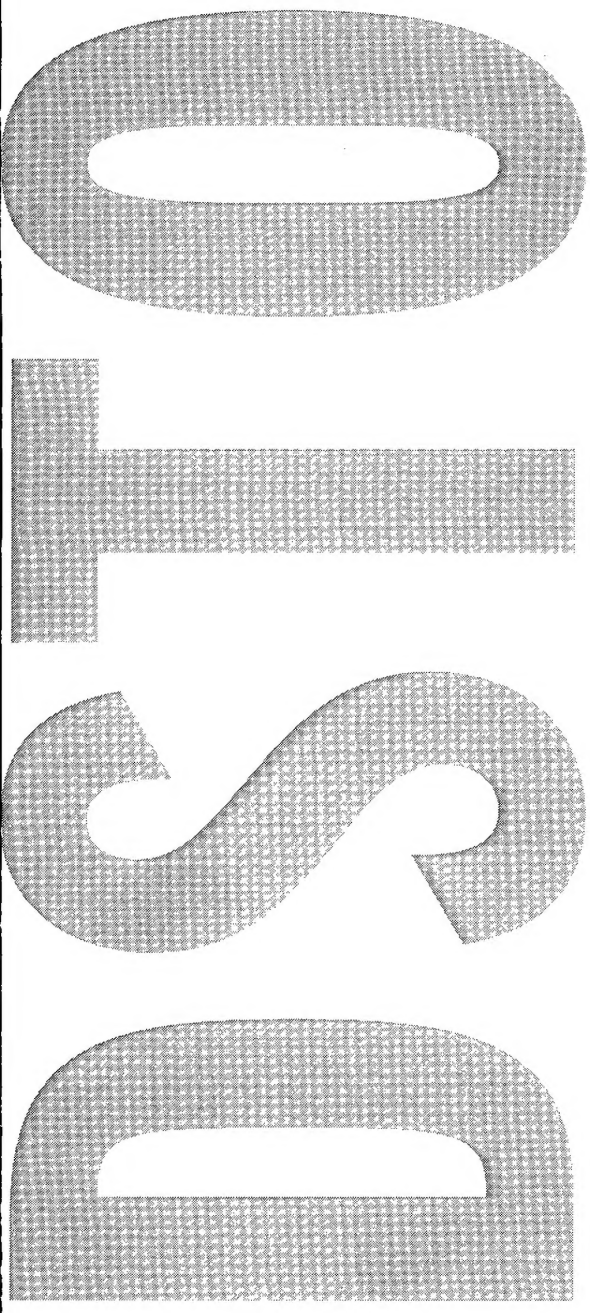
DEPARTMENT OF DEFENCE
DEFENCE SCIENCE & TECHNOLOGY ORGANISATION
DSTO



A Concept of Defence Core Communication Infrastructure Supporting M-QoS

Marek Kwiatkowski

DSTO-TR-1220

A Concept of Defence Core Communication Infrastructure Supporting M-QoS

Marek Kwiatkowski

Communications Division
Electronics and Surveillance Research Laboratory

DSTO-TR-1220

ABSTRACT

This report is a continuation of DSTO's research effort in the area of Military oriented Quality of Service (M-QoS) and presents an architectural concept of network transmission, control and management that would offer M-QoS features over the Defence terrestrial/satellite Core communications infrastructure. The report first discusses in more detail the use of the transmission framework proposed in an earlier study by the same author, with particular emphasis put upon IP Differentiated Services - a vital technology to implement M-QoS. Then, a Military oriented Network Control and Management (M-NC&M) framework, based on policy-enabled networking and bandwidth brokerage that would facilitate the implementation of M-QoS is described. The M-NC&M framework utilises results from the IETF's standardisation effort on policy framework and work from the Internet2 on bandwidth brokerage. Finally, a number of future research studies supporting the architectural concept are proposed in the report.

DEPARTMENT OF DEFENCE
DEFENCE SCIENCE & TECHNOLOGY ORGANISATION
DSTO

Published by

DSTO Electronics and Surveillance Research Laboratory
PO Box 1500
Edinburgh, South Australia 5108, Australia

Telephone: (08) 8259 5555
Fax: (08) 8259 6567

AR-012-032
October 2001

Author

Dr Marek Kwiatkowski
Communications Division

Dr Marek Kwiatkowski received the M.Sc. degree from the Silesian Technical University, Gliwice, Poland, in 1979 (Computer Science), and the Ph.D. degree from AGH, Cracow, Poland, in 1990 (Telecommunications). From 1991 until 1998, he worked at the Teletraffic Research Centre, University of Adelaide, first as a Post Doctoral Fellow, and from 1995 as a Research Fellow. Since June 1998 he has been working at the DSTO, Network Integration Group, as a Senior Research Scientist. His main research interests include control and management aspects of multimedia military and commercial networks.

A Concept of Defence Core Communication Infrastructure Supporting M-QoS

Executive Summary

This report presents a concept of network transmission, control and management architecture that would offer Military oriented Quality of Service (M-QoS) features over the Defence terrestrial/satellite Core environment communications infrastructure.

The term M-QoS represents commercial QoS in conjunction with the following three main features. Firstly, in military packet networks, when not enough network resources are available to support hard QoS for all traffic flows, the flows carrying mission critical information should get preference (i.e., higher priority) over less important flows. Secondly, in overloaded networks, it is preferable to gracefully "step down" the hard QoS of less important military flows instead of automatically tearing down these flows. Finally, higher flow priorities should be given for a restricted time defined by doctrine. Today's packet based ADF networks do not support M-QoS.

The subset of the long-distance Defence Core communication environment chosen for the analysis within the report is composed of: (1) Packet oriented fixed (terrestrial) networking infrastructure (called fixed network for short), used for strategic communications and composed of the Backbone Routing Service (BRS), the Secure Backbone Routing Service (SECBRS) and the Defence Corporate Backbone Network (DCBN); and (2) Packet oriented satellite infrastructure used to: (a) interconnect the fixed network with a tactical trunk network; and (b) provide back-up connectivity for the fixed network. The report is focused on using this environment for Local Area Networks (LANs)/Base Area Networks (BANs) connectivity. It is noted that the chosen environment is becoming crucial in carrying bulk Defence multimedia traffic.

The report addresses short to medium term (2-5 years) design goals.

The following three basic components involved in delivering M-QoS can be identified: (a) a standardised M-QoS interface between a military end-user application and the network management and control; (b) transmission infrastructure, which supports (commercial) QoS features; and (c) military oriented network control management.

Previous DSTO studies have mainly been related to the design of a standardised M-QoS interface and to a preliminary assessment of some promising available or emerging commercial transmission technologies regarding their potential support of M-QoS.

This report firstly discusses in more detail the previously chosen transmission technologies with particular emphasis placed upon IP Differentiated Services, which, as argued in the report, is a vital technology to implement M-QoS. Typical DiffServ functions such as packet classification, marking, metering, dropping, shaping and queueing are analysed in regard to their roles in offering M-QoS. Since Defence uses

primarily Cisco routers, the report also attempts to identify Cisco's solutions to provide these functions.

Secondly, the report presents a concept of a Military oriented Network Control and Management (M-NC&M) framework that would facilitate the implementation of M-QoS.

Finally, a number of future research studies supporting the architectural concept are proposed in the report.

The most important findings of this report are as follows:

a. M-QoS can likely be implemented in a scalable and flexible way in the Defence terrestrial/satellite Core using a set of transmission technologies identified in a previous report (i.e., IPv4/IPv6, Differentiated Services, MPLS and ATM) in conjunction with bandwidth brokerage and Policy-based Network Management;

b. In the area of transmission technologies, the most challenging Defence-specific issues requiring further study are mappings between DiffServ, MPLS and ATM technologies to implement M-QoS and traffic engineering using MPLS to support M-QoS;

c. The IETF's policy framework can be useful when implementing M-QoS oriented network management;

d. The Internet2's QBone bandwidth broker (BB) architecture seems to be generic enough to implement desirable control/management functions supporting M-QoS. However, the concepts developed for other bandwidth broker architectures should also be considered.

Based on the report's findings, the following is recommended:

A. Continue to monitor the progress within:

- The IETF policy-enabled network management architecture and its commercial developments;
- The Internet2's QBone and other bandwidth broker management architectures and their commercial developments.

B. Undertake in the near term the following studies:

- Analysis of the role of policies in future Defence network management;
- Specification of high-level policy examples for Defence;
- Specification of the detailed BB architecture including design of viable flow admission control algorithm(s) and performance monitoring;
- Analysis of inter-domain brokerage including performance issues pertaining to satellite bearers.

Contents

1. Introduction

This report presents a concept of network transmission, control and management architecture that would offer M-QoS features over the Defence terrestrial/satellite Core communications infrastructure.

The report is a continuation of the research effort in the area of Military oriented Quality of Service (M-QoS) presented in [KWIA99a, BLAC00, KWIA01]. To help the reader, the basics of the M-QoS concept are repeated in Appendix A.

Fig. 1 shows the basic components involved in delivering M-QoS. These include:

- A *standard M-QoS interface* between a military end-user application and network management and control (see Appendix A for more details);
- *Transmission infrastructure*, which supports (commercial) hard/soft QoS[1] features;
- *Military oriented Network Management and Control*, which provides flow admission control, reserves network resources for the flows, and monitors network health.

The issues related to a standard M-QoS interface are addressed in [BLAC00, GEOR01]. Basic properties of the interface within the context of policy-enabled military networks, including the Service Level Specification (SLS)[2] are described in [BLAK00]. Robust software for the interface when used in a Defence IP-oriented environment is presented in [GEOR01].

General aspects of the long-distance transmission infrastructure are addressed in [KWIA01] where the suitability of promising commercial transmission technologies (both existing and emerging) to support M-QoS in a subset of the Defence Core is preliminarily assessed. The document proposes the use of a combination of IPv4/IPv6, Differentiated Services (DiffServ), Multi-protocol Label Switching (MPLS) and ATM upon which the M-QoS would be implemented, as depicted in Fig. 2.

In relation to Military oriented Network Management and Control, the same document suggests the use of policy based network management and bandwidth brokerage[3] to support the implementation of DiffServ (see Fig. 2).

---

[1] The terms hard/soft QoS are defined in Appendix A.

[2] An SLS is a set of parameters and their values which together define the service offered to a traffic stream by a DiffServ domain [GROS01].

[3] Bandwidth brokerage augments DiffServ with the capability to perform flow admission control and automate network resource management.

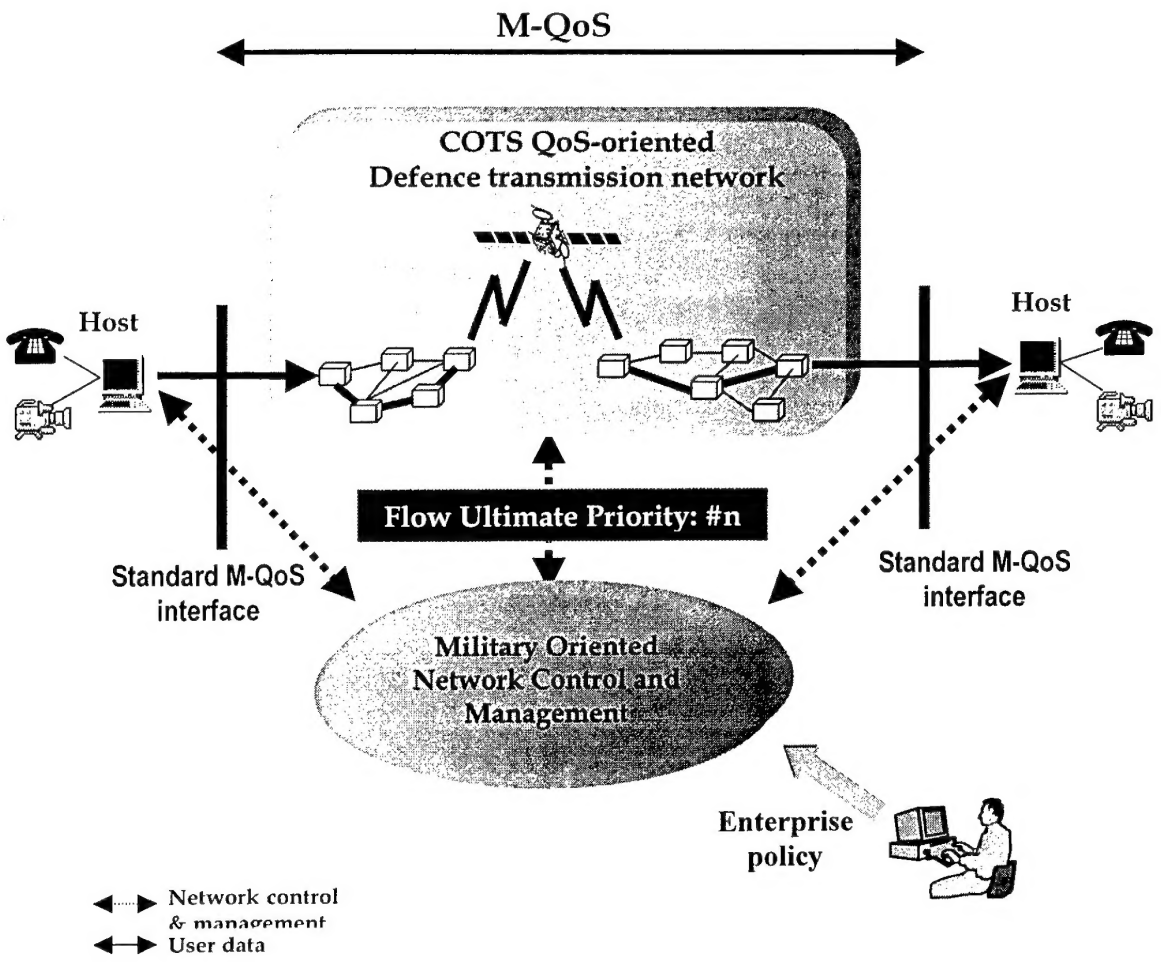


Fig. 1 The M-QoS concept [KWIA01].

The aims of this report are as follows:

1. Discuss in more detail the use of the transmission technologies proposed in [KWIA01], with particular emphasis put upon DiffServ, being the vital technology to implement M-QoS;
2. Propose a concept of Military oriented Network Control and Management (M-NC&M) that facilitates the implementation of M-QoS through the use of policy enabled networking and bandwidth brokerage;
3. Identify future research areas for (1,2).

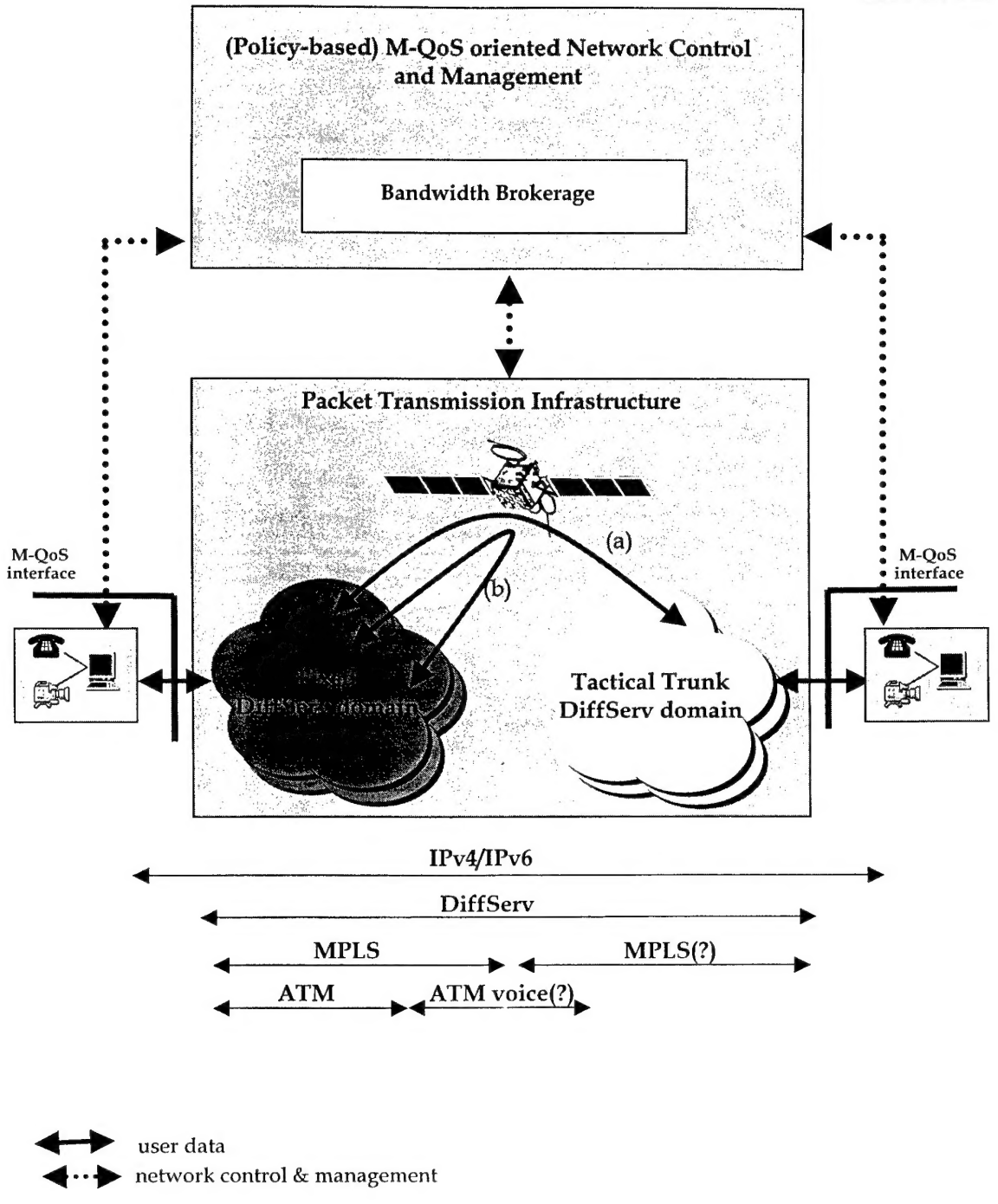


Fig. 2 The combination of transmission technologies and the supporting network control and management as proposed in [KWIA01]. (BB – Bandwidth Broker, (a) connectivity between the fixed and tactical trunk networks, (b) back-up trunks to the fixed network.)

As in [KWIA01], The subset of the long-distance Defence Core communications environment chosen for the analysis is composed of:

a. *Packet oriented fixed (terrestrial) networking infrastructure,* used for strategic communications and composed of the Backbone Routing Service (BRS), the Secure Backbone Routing Service (SECBRS) and the Defence Corporate Backbone Network (DCBN) (see [BLAC01] for details). In this report, this infrastructure will be called *fixed network* for short.

b. *Packet oriented satellite infrastructure,* used to:

   - interconnect the fixed network with a *tactical trunk network*[4] (e.g., used by deployed headquarters), as depicted by (a) in Fig. 2;
   - provide back-up connectivity for the fixed network, as depicted by (b) in Fig. 2.

Note that the chosen environment becomes crucial in carrying bulk Defence multimedia traffic. For the sake of simplicity, whenever the term *Core* is further used in this report, it will mean the above-specified subset of the Core.

Also, as in [KWIA01], this report is focussed on the use of the Core for Local Area Networks (LANs)/Base Area Networks (BANs) inter-connectivity. The report assumes that these LANs/BANs do not impose any internal problems in providing hard/soft QoS to end-user applications due to the abundance of available bandwidth.

The report addresses short to medium term (2-5 years) design goals.

The structure of the report is as follows. Section 2 presents a more detailed discussion of the transmission technologies proposed in [KWIA01] in relation to their potential use in the Defence Core. A concept of Military oriented Network Control and Management (M-NC&M) that facilitates the implementation of M-QoS using policy enabled networking and bandwidth brokerage is described in Section 3. The summary of the report's findings and recommendations are presented in Section 4.

[4] It is noted that other components of a tactical network such as a Combat Net Radio sub-system are beyond the scope of this report.

2. Packet Transmission Framework

2.1 General remarks

This section describes in more detail the packet transmission model shown in Fig. 2. Particular attention will be given to DiffServ since this service will be crucial in providing hard/soft QoS, prioritisation of IP flow aggregates, as well as graceful degradation in hard QoS of flows.

2.2 IPv4/IPv6

As stated in [KWIA01], IPv4/IPv6 will generally be used for end-to-end communication across the (terrestrial/satellite) Defence Core between end-user applications to transfer multimedia information. The only possible exception is provision of real time, low jitter services (e.g., voice) over slow satellite links. ATM may need to be used instead (see discussion in [KWIA01]).

The inclusion of IPv6 is due to the expected gradual replacement of IPv4 by the newer version, rather than because of its specific QoS features.

2.3 DiffServ

Core routers will be divided into a number of DiffServ domains as shown in Fig. 2. The number and the size of fixed network domains require further study. In the case of the tactical environment, it is expected that each tactical trunk subsystem will form a single DiffServ domain.

Routers in a DiffServ domain will implement a number of Per-hop Behaviours (PHBs)[5], each having a distinct DiffServ Code Point (DSCP) value. A maximum number of 64 PHBs can be created. A PHB Group is a set of one or more PHBs, which can only be implemented simultaneously, due to a common constraint applying to all PHBs in the set [NICH98]. Fig. 3 presents router classifications as used in [KWIA0]. Note that a single router may perform functions of different router types at the same time.

In the proposed framework, it is strongly suggested that all Core routers in a domain implement PHBs and PHB Groups in a consistent way. The parameters such as the number of PHBs, their characteristics and groupings will be decided in a relatively static fashion through an enterprise policy. An example of how these parameters can be set is given in Section 2.3.7. To implement a PHB, DiffServ domain routers will use packet classification, marking, metering, dropping, shaping and queueing mechanisms, as generically depicted in Fig. 4. It is noted that DSTO is currently conducting experiments with various configurations/arrangements of these features.

[5] A PHB characterises the externally observable forwarding treatment applied at a DiffServ-compliant router to a collection of packets.

Below, we discuss these mechanisms in relation to our M-QoS framework. Since Defence uses primarily Cisco routers, we will also refer to Cisco's solutions when presenting the mechanisms.

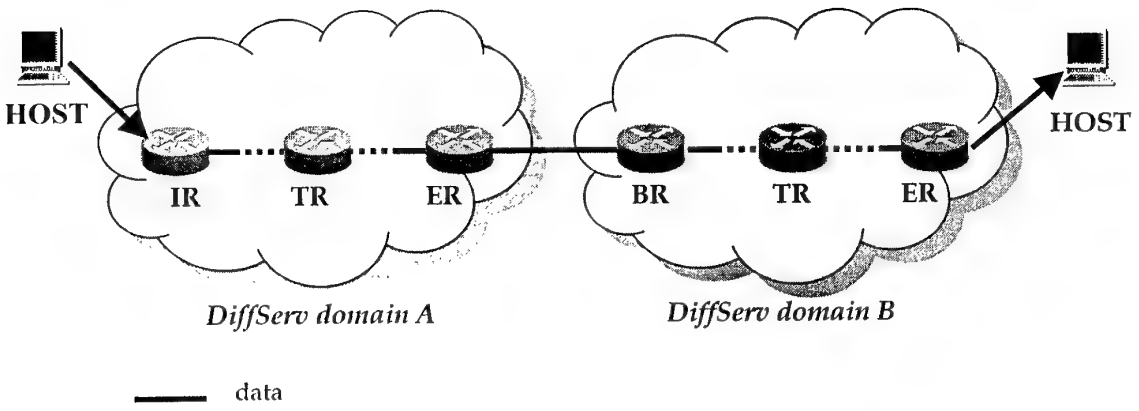


Fig.3. DiffServ domains (IR – ingress router, TR – transit router, BR – boundary router, ER – egress router.)

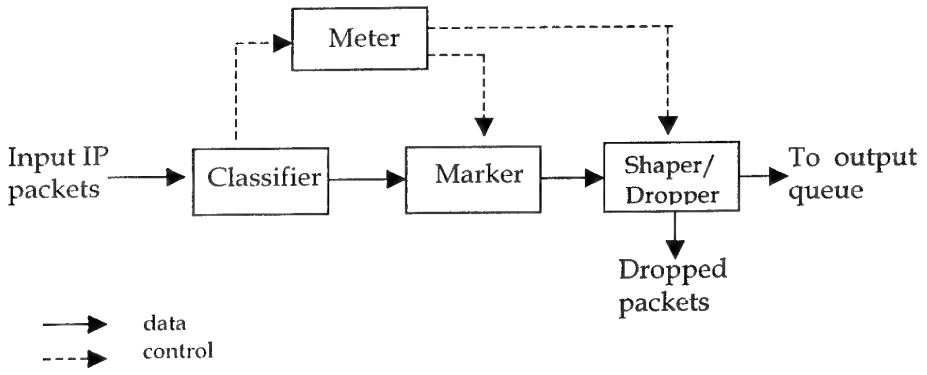


Fig. 4. A block diagram representing DiffServ functions in a router.

2.3.1 Packet classification

Packets entering a router will be classified to one of the specified PHBs using filters. Cisco routers offer various methods to create such filters, including Access Control Lists (ACLs) and Network-based Application Recognition (NBAR) [CISC01].

Our concept assumes that packets sent from end-user applications to ingress routers (IRs) will be classified based on the carried DSCP value or using the 5-tuple (Source IP address, Source Port number, Destination IP address, Destination Port number, and possibly the transport protocol). The former case applies to situations where trusted hosts (e.g., Defence servers) send packets with set DSCP values. The latter case refers to packets sent from non-trusted hosts. The rules for classifying a flow[6] in IRs will be imposed in a dynamic fashion by the domain's Bandwidth Broker during flow admission.

All routers other than the ingress ones (i.e., transit, egress and boundary routers – see Fig. 3) will classify packets using the packet's DSCP value set by the markers (see below) in ingress routers. The filters in transit/egress/boundary routers will be statically configured by network management at the time of configuring router resources for PHBs.

2.3.2 Packet metering

Packet metering is used to measure temporal properties of a flow/flow aggregate selected by the classifier against a traffic profile specified in a Service Level Specification (SLS) and/or against any relevant policy requirements. The results of metering are then sent to a marker and shaper/dropper (see Fig. 3) to trigger a desirable action for in/out-of profile packets. In Cisco routers metering is performed using a token bucket algorithm.

In our concept, the rules for metering a flow incoming from end-user applications to ingress routers will be specified by BBs at the time of admitting the flow. The rules for metering classes of traffic will be imposed at the time of configuring the classes by M-NC&M.

2.3.3 Packet marking

Marking is the process of setting the DSCP value in a packet based on defined rules [BLAK98]. In our approach, packets containing user information can be marked either by trusted hosts (see section 2.3.1) or by ingress routers based on results of packet

[6] In this report, the term *flow* corresponds to the term *microflow* used by IETF [NICH98].

classification and metering. The rules for marking will be specified by BBs at the time of admitting flows.

Changing the marking in the Core of already marked packets is not foreseen.

2.3.4 Packet dropping

This process, also called *policing*, aims at discarding packets based on information provided by meters, and according to the rules specified by BBs. In Cisco routers, dropping is achieved using the Committed Access Rate (CAR) mechanism applied on an interface basis.

In our concept, policing in ingress routers will be applied to all military-essential flows admitted by BBs. BBs will be responsible for sending to the routers a specification of dropping rules. This policing will be crucial to assure conformance of traffic sent by end-user applications to the Service Level Specifications (SLS) negotiated during flow admission.

It is stressed that individual best-effort flows will not be policed.

2.3.5 Packet shaping

Packet shaping is a process of delaying packets within a packet stream to conform to some defined traffic profile. Cisco routers offer Generic Traffic Shaping (GTS) to do the shaping.

At the time of writing, it is not clear whether and to what extent packet shapers will be required in the proposed transmission architecture. This requires further study.

2.3.6 Packet queueing

The report proposes the use of packet queueing that will enable:

- *Use of up to 64 PHBs of traffic;*
- *Grouping of PHBs into PHB Groups, each having a separate output queue;*
- *Use of Random Early Detection (RED) mechanism* - this mechanism helps to avoid global synchronisation of TCP flows - an undesirable feature of using tail dropping during congestion. RED randomly instead drops packets from a queue past a certain threshold. This forces the TCP "slow start" to only a small number of IP flows;
- *Allocation of a minimum guaranteed bandwidth per each PHB Group* – this feature prevents bandwidth starvation of any PHB Group;
- *Automatic allocation of unused bandwidth to other classes that need it* – this feature provides efficient use of bandwidth;

- *Ability to offer absolute priority to some chosen classes* - this feature is crucial to implement real-time, low jitter traffic (e.g., voice).

In regard to Cisco routers, a combination of the following mechanisms covers the above listed features [CISC00]:

- *Class Based Weighted Fair Queueing (CBWFQ).*

  This discipline enables the definition of up to 64 PHBs. PHBs can be grouped into classes (i.e., PHB Groups), each having assigned a minimum guaranteed bandwidth during congestion, weight and maximum length. The weight of a packet belonging to a specific class is derived from the minimum bandwidth assigned to the class. If a queue reaches its configured queue limit, enqueueing of additional packets to the class causes tail drop;

- *Weighted Random Early Detection (WRED).*

  This mechanism is a combination of RED and DSCP. With WRED, separate thresholds triggering dropping are maintained for packets with different IP precedence[7] values. In this way, preference in dropping can be given to some PHBs over others using the same queue.

- *Low Latency Queueing (LLQ).*

  When used with CBWFQ, LLQ allows delay-sensitive data such as voice to be sent first before packets in other queues, thus giving delay-sensitive data preferential treatment over other traffic [CISC00]. A single strict priority queue is maintained for the LLQ traffic. One or more traffic classes can be nominated to carry delay-sensitive traffic. For the latter, all the traffic goes to a single LLQ queue instead of class queues.

Our framework assumes that all Core routers will have all the above features implemented.

2.3.7 Flow admission control

As stated in [KWIA01], since DiffServ does not provide a direct QoS interface with end-user applications, a special entity called a *Bandwidth Broker* (BB) can be used to facilitate automatic Service Level Specification (SLS) arrangements. The discussion of how bandwidth brokerage can be designed to support M-QoS is presented in Section 3.

[7] IP Precedence is specified by the value of DSCP bits 0-2.

2.3.8 Case scenario

The following scenario represents a plausible application of DiffServ to differentiate military traffic flows across an operational network. The following assumptions are made:

- All communication is divided into three broad types: (1) non-military essential; (2) military-essential; and (3) network control and management. The non-military essential traffic is treated as best effort. The military essential traffic is composed of the following categories: (a) formal messaging; (b) land related missions; (c) sea related missions; (d) air related missions; (d) intelligence;
- The following traffic types are distinguished for each category: (a) voice; (b) real time VBR (e.g., streaming video); (c) bulk data transfer (e.g., formal messaging, FTP, HTTP); and (d) interactive (e.g., Telnet). Network control and management constitutes a separate traffic type;
- Except for voice, each traffic type has four precedence levels: (a) routine; (b) priority; (c) immediate; and (d) flash. Different dropping probabilities should be applied to these precedence levels.

Table 1 shows a possible solution of the problem using mechanisms offered by Cisco to implement DiffServ.

PHB #	Cisco Output Class #	PHB Group #	Communication type/ traffic category	Traffic Type	Military Precedence
1	1 (default)	1	Non-military essential	Best effort	N/A
2	2	2	Formal messaging	Bulk data	N/A
3	3	3	Land	voice	N/A
4	4	4 + WRED	Land	RT VBR	routine
5	4	4 + WRED	Land	RT VBR	priority
6	4	4 + WRED	Land	RT VBR	immediate
7	4	4 + WRED	Land	RT VBR	flash
8	5	5 + WRED	Land	interactive	routine
9	5	5 + WRED	Land	interactive	priority
10	5	5 + WRED	Land	interactive	immediate
11	5	5 + WRED	Land	interactive	flash
12	6	6 + WRED	Land	bulk data	routine
13	6	6 + WRED	Land	bulk data	priority
14	6	6 + WRED	Land	bulk data	immediate
15	6	6 + WRED	Land	bulk data	flash
16	7	3	Sea	voice	N/A
17	8	7 + WRED	Sea	RT VBR	routine
18	8	7 + WRED	Sea	RT VBR	priority

19	8	7 + WRED	Sea	RT VBR	immediate
20	8	7 + WRED	Sea	RT VBR	flash
21	9	8 + WRED	Sea	interactive	routine
22	9	8 + WRED	Sea	interactive	priority
23	9	8 + WRED	Sea	interactive	immediate
24	9	8 + WRED	Sea	interactive	flash
25	10	9 + WRED	Sea	bulk data	routine
26	10	9 + WRED	Sea	bulk data	priority
27	10	9 + WRED	Sea	bulk data	immediate
28	10	9 + WRED	Sea	bulk data	flash
29	11	3	Air	voice	N/A
30	12	10 + WRED	Air	RT VBR	routine
31	12	10 + WRED	Air	RT VBR	priority
32	12	10 + WRED	Air	RT VBR	immediate
33	12	10 + WRED	Air	RT VBR	flash
34	13	11 + WRED	Air	interactive	routine
35	13	11 + WRED	Air	interactive	priority
36	13	11 + WRED	Air	interactive	immediate
37	13	11 + WRED	Air	interactive	flash
38	14	12 + WRED	Air	bulk data	routine
39	14	12 + WRED	Air	bulk data	priority
41	14	12 + WRED	Air	bulk data	immediate
42	14	12 + WRED	Air	bulk data	flash
43	15	3	Intelligence	voice	N/A
44	16	13 + WRED	Intelligence	RT VBR	routine
45	16	13 + WRED	Intelligence	RT VBR	priority
46	16	13 + WRED	Intelligence	RT VBR	immediate
47	16	13 + WRED	Intelligence	RT VBR	flash
48	17	14 + WRED	Intelligence	interactive	routine
49	17	14 + WRED	Intelligence	interactive	priority
50	17	14 + WRED	Intelligence	interactive	immediate
51	17	14 + WRED	Intelligence	interactive	flash
52	18	15 + WRED	Intelligence	bulk data	routine
53	18	15 + WRED	Intelligence	bulk data	priority
54	18	15 + WRED	Intelligence	bulk data	immediate
55	18	15 + WRED	Intelligence	bulk data	flash
56	20	17	Network control and management	N/A	N/A

Table 1. An example of applying DiffServ to differentiate military traffic flows. (PHB – Per Hop Behaviour, WRED - Weighted Random Early Detection.)

Each PHB in Table 1 has an associated unique DSCP. All PHBs representing the same traffic type and mission group are allocated to the same class. Each class has allocated

minimum bandwidth. All voice classes are mapped to a single LLQ queue. All other classes have separate queues. Different military precedence levels are mapped to separate IP precedence bits. Note that the use of IP precedence bits to reflect military precedence is advantageous when DiffServ is supported by MPLS (see next section), since IP Precedence can be mapped one-to-one onto Experimental Bits in the MPLS header.

Best Effort traffic represents the default CBWFQ class. Flow based Weighted Fair Queueing (WFQ) can be used for this class. WFQ ensures that bandwidth available for the class is shared fairly between individual conversations and that low-volume (e.g., Telnet) traffic is timely transferred.

Note that there are 8 unused DSCP codes in the proposed scenario.

2.4 MPLS

In the proposed transmission framework, MPLS will be used to provide more predictable DiffServ. It will mainly be utilised within the (terrestrial) fixed network and possibly over a satellite to provide back-up links (depicted as (b) in Fig. 2) to the fixed (strategic) network, thus increasing its survivability. The use of MPLS is also envisaged between the fixed and tactical trunk networks (depicted as (a) in Fig. 2) in the case when more than single satellite connectivity exists between two sites.

MPLS will be applied to achieve:

a. *Precise control of IP traffic.*

   Different treatment can be applied to better separate DiffServ traffic classes through mapping them to different Label Switched Paths (LSPs). These paths may have different attributes (e.g., traffic parameter attributes, generic path selection and maintenance attributes – see [AWDU99]) impacting the QoS experienced by packets.

   There are potentially a number of ways of mapping DiffServ classes described in the previous section onto LSPs. A potential solution could be to map each PHB group into a separate LSP. In this case, IP Precedence bits can be mapped one-to-one into Experimental Bits in the MPLS header, thus providing a consistent treatment of PHBs across both DiffServ and MPLS infrastructures.

b. *Foundation for traffic engineering.*

   This feature enables the network to direct traffic flows using routes which are less congested, and not necessarily the least-cost ones, a typical approach used by Interior Gateway Protocols (IGPs) such as OSPF or IS-IS;

c. *Rapid QoS restoration after a network failure.*

   In the case of single or multiple failures in the primary path, traffic can be precisely rerouted, either using a new established or a hot standby LSP(s).

d. Building Virtual Private Networks (VPNs).

MPLS can be used to build scalable IP VPNs through supporting any-to-any (i.e., full mesh) communication among all the sites without the need to build a full-mesh ATM PVC network. This might be an important feature for the Defence Core characterised by a large number of potential VPN sites and routes.

The details relating to how MPLS could be utilised in the Defence Core needs further study. It is expected, however, that the MPLS solutions supporting DiffServ emerging commercially will likely satisfy Defence needs. An exception might be the use of MPLS over satellite links - a very new research area.

It is noted that both Cisco [CISC00a] and Nortel [NORT00] support MPLS.

2.5 ATM

Our transmission network concept assumes that ATM will still be used in the terrestrial part of the Defence Core Backbone Network for the foreseeable future. Firstly, it will support MPLS switching. The way(s) MPLS should be mapped onto ATM requires further study. However, it is anticipated that the protocol stack composed of IP over MPLS over ATM will gradually be replaced by IP over Sonet/SDH or even IP directly over fibre. These new technologies will be supported by the Generalised Multi-Protocol Label Switching (GMPLS)[8] [ASHW01] instead of MPLS.

Secondly, ATM will continue to carry voice traffic in the terrestrial part of the Core until VoIP is implemented on a large scale. As stated in [KWIA01], ATM cells (but not necessarily the control plane) may be required to transport voice over slow satellite links if IPv4/IPv6 and DiffServ do not satisfy the low jitter requirements.

2.6 Final remarks

We have shown that IPv4/IPv6, DiffServ, MPLS and ATM are the transmission technologies that would likely enable to implement M-QoS in a scalable and flexible way within the Defence terrestrial/satellite Core.

The most challenging Defence-specific issues requiring further study are:

- Mappings between DiffServ, MPLS and ATM technologies to implement M-QoS;
- Traffic engineering using MPLS to support M-QoS.

[8] GMPLS is a development of MPLS currently being investigated by the IETF.

3. Network Control and Management Framework

3.1 General remarks

As generally stated in Section 1, our concept of M-NC&M is based on the use policy enabled network management and bandwidth brokerage. As to the former, a review of policy enabled network management efforts can be found in [BLAC00]. Our approach utilises the results of the IETF's standardisation effort on policy framework [POLI].

As to bandwidth brokerage, there are a number of research and experimental activities worldwide, including the Aquila project [STEL00] led by Siemens, the GARA project [GARA00] involving a number of US universities and the QBone project [QBONE] being a part of the Internet2[9] effort. The latter is probably the most promising, and our approach utilises a number of ideas proposed within the QBone project.

The next two sections present the IETF's policy framework and the Internet2's QBone project in more detail followed by description of the proposed M-NC&M concept.

3.2 IETF's policy framework

Policy is a way of allocating network resources (e.g., the buffers in a router, bandwidth on an interface) to services (e.g., DiffServ) in terms of enterprise decisions. It is composed of one or more rules that describe the action(s) to occur when specific condition(s) exist [STAR99].

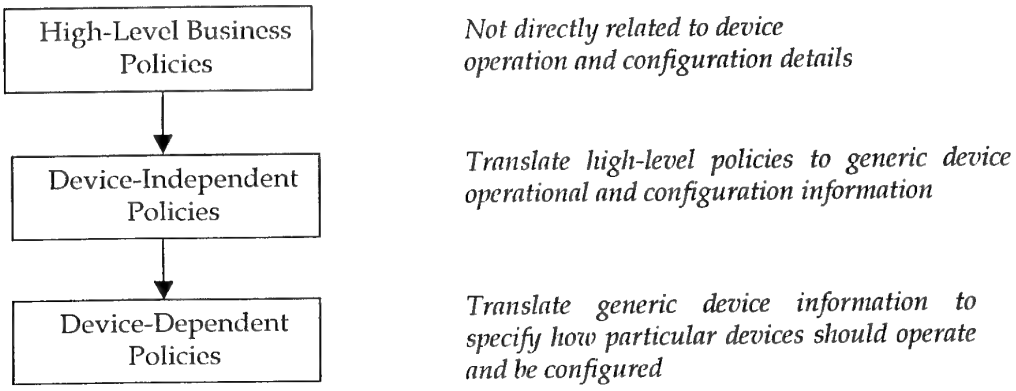


Fig. 5. A general model for translating policies [MOOR01b].

[9] Internet2 is a collaborative effort to develop advanced Internet technology and applications for research and higher education [INTE201].

The IETF's Policy Framework Charter [POLI01], Differentiated Services Charter [DIFF01] and Resource Allocation Protocol Charter [RAP01] are currently working on a framework that would enable network administrators to represent, manage, share, and reuse policies and policy information in a vendor-independent, interoperable, and scalable manner. Particular focus of this effort is to address the needs of QoS traffic management.

A general model for translating policies is presented in Fig. 5, and the primary components of the IETF policy framework are shown in Fig. 6, including:

- *Policy Decision Point (PDP)* - also called a *policy server,* makes decisions using policies retrieved from a policy repository and possibly from other locations such as authentication server;
- *Policy Enforcement Point (PEP)* - actually enforces the policy decisions in network nodes;
- *Policy repository* - is a data store (e.g., database, directory) that holds policy rules and related data.

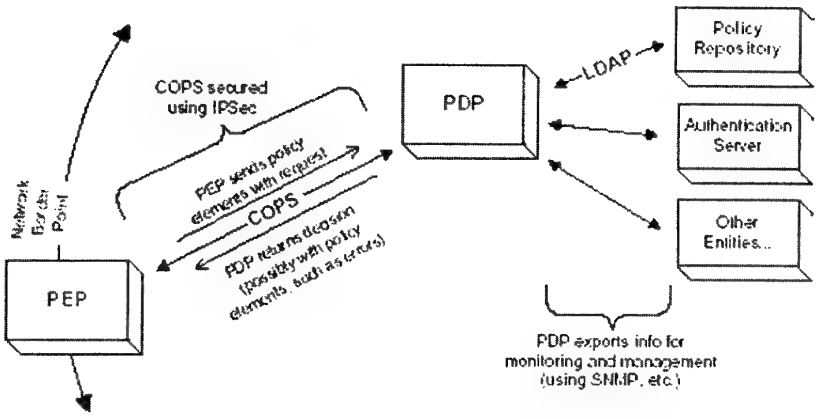


Fig. 6. The IETF policy framework [STAR99]. (LDAP – Lightweight Directory Access Protocol, COPS - Common Open Policy Service, SNMP – Simple Network Management Protocol)

The separation of PEP, PDP and policy repository presented in Fig. 6 is logical rather than physical. That is, the components may be built into a single physical device. A number of PEPs may be related to a single PDP, and a number of PDPs may exist within a system

Fig. 6 also identifies typical protocols used for communication between the framework components. A special protocol called *Common Open Policy Service* (COPS) [CHAN01] has been designed to facilitate the efficient exchange of policy information between a

PDP and its clients (i.e., PEPs). COPS is a simple, scalable, query/response TCP-based protocol. It has been designed to support multiple types of policy clients. Currently, two common models are supported: *outsourcing* and *provisioning*. The outsourcing model, also called COPS-RSVP [HERZ00], assumes that a PEP sends a COPS request message to the PDP if it receives an RSVP message requiring a policy decision. The PDP then sends back its decision using COPS Decision message. In other words, there is a direct one-to-one correlation between PEP requests and PDP decisions. In the provisioning model (also called COPS-PR) which addresses the use of policies in the DiffServ environment, there is generally no correlation between PEP requests and PDP decisions. That is, the PDP may proactively provision the PEP reacting to external events (e.g., user input), PEP events, and any combination thereof [COPS-PR]. It is noted that COPS-PR may be used for the configuration of different types of network services including MPLS, Security, VPN and VoIP [IPHWY01].

It is important to note that COPS is not mandated by the IETF policy framework. There are currently very few COPS-compliant PEPS available commercially. As a result, protocols such as SNMP, CLI and HTTP are commonly used to communicate between a PDP and a PEP.

Another protocol mentioned in Fig. 6 is Lightweight Directory Access Protocol (LDAP), a low-cost protocol to access policies stored in directories supporting X.500 models [WAHL97].

Note that the IETF in its standardisation work has not yet addressed bandwidth brokerage support to DiffServ.

3.3 Internet2's research on bandwidth brokerage

This research is conducted by the QoS Working Group within its flagship project called QBone which is an effort to specify, deploy, and evaluate new IP services in an interdomain DiffServ testbed.

The group has developed a draft general architecture, described in [TEIT99a, TEIT99b], for the QBone testbed. This architecture assumes the use of DiffServ domains, which will deliver the Expedited Forwarding (EF)[10] and Best Effort (BE) Per-Hop Behaviours (PHBs). Each domain will manage its own resources using a bandwidth broker as shown in Fig. 7. The term "bandwidth broker" (BB) refers here to the abstraction that automates admission control and to a lesser degree configuration functionality.

Some preliminary work has been done by the group to develop an integrated measurement architecture which defines a basic set of metrics (e.g., one-way packet loss, one-way packet delay variation, link utilisation) to be collected at each ingress and egress router of a QBone domain, as well as dissemination and presentation

[10] This PHB has been designed to provide the highest QoS, which offers low delay, low jitter, low loss and assured bandwidth by (almost) precluding any queueing at routers, regardless of the load they experience [JACO99]

requirements for these data sets [TEIT99b]. Note that the group is currently revising this architecture.

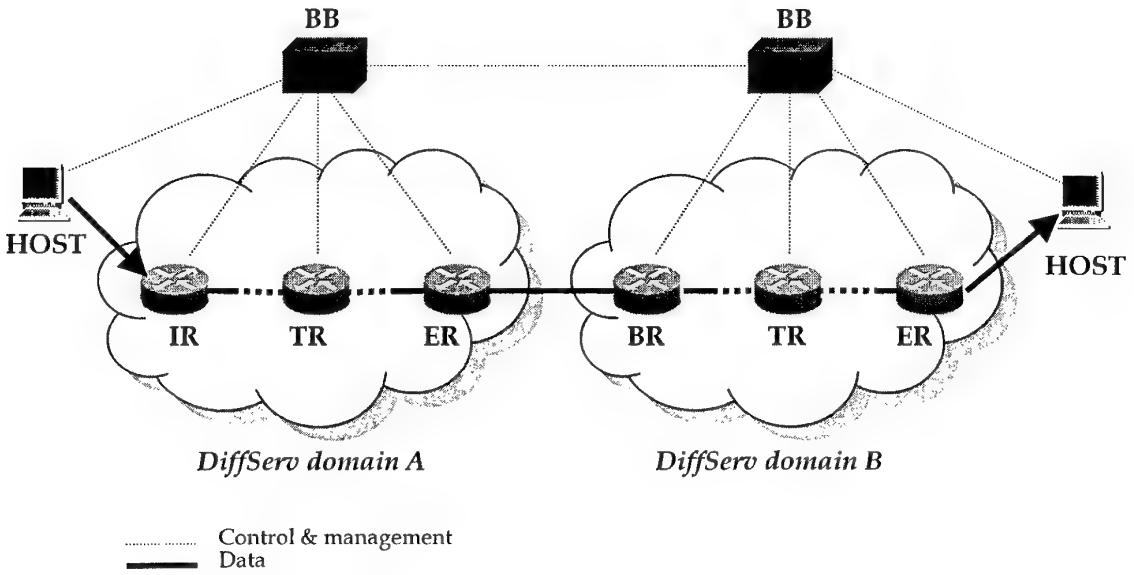


Fig. 7. QBone multidomain architecture. (IR – ingress router, TR – transit router, BR – border router, ER – egress router, BB – Bandwidth Broker.)

A separate effort is being devoted by the group to develop a bandwidth broker architecture for QBone [QBONEa]. In this architecture, shown in Fig. 8, the routing tables (depicted as *routing info* in Fig. 8) may contain both inter-domain and intra-domain information used to determine the flow path inside and between domains, respectively. The *Data Store* contains data, which is common for all BB components, including: (a) SLS information for all ingress/egress routers; (b) current reservations and resource allocations; (c) configurations of routers; (d) policy information pertinent to bandwidth brokerage; (e) network management information; and (f) monitoring information from routers. Interfaces with other entities (depicted as *NMS iface* in Fig. 8) such as network management system and policy management enable the separation of network management functions (e.g., configuration management) between the BB, the policy administration and the network management system.

Note that not all the components presented in Fig. 8 need to be used in every implementation.

Network management protocols such as SNMP and COPS are planned for the communication between a BB and a router. The use of RSVP is being considered for the communication between a BB and a host. Finally, a specially designed protocol, called Simple Interdomain Bandwidth Broker Signalling (SSIBS), is being developed for the communication between BBs.

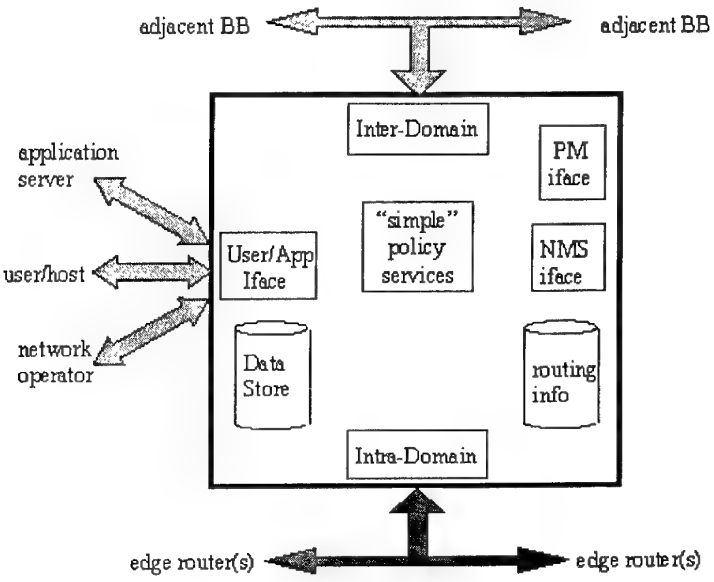


Fig. 8. Functional decomposition of the QBone bandwidth broker [QBONEa]. (PM – policy management, NMS – network management system, iface – interface.)

Both individual and aggregate flow reservations are possible in the QBone architecture. The former works as follows. The source end-user application first sends to its home BB the SLS of the requested flow. The BB authenticates the request and then assesses whether the flow can be admitted based on the amount of free resources (e.g., link bandwidth, buffers) available in its domain. If the amount is sufficient, the request is sent either to the destination end-user application for approval if the request involves only this single domain, or the request is sent (using SSIBS) to the next BB in the chain if a multi-domain reservation is required. Each BB and the destination end-user application may refuse the request. However, if all of them approve the request, the home BB orders the ingress (edge) router to classify, mark and police all the packets belonging to the flow according to the agreed SLS. Then the BB informs the end-user application that it can start sending packets. Either the end-user application or any involved BBs may release the reservation.

The presented flow admission is scalable firstly because the reservation requests are made only for flows which require better than best-effort quality, and secondly because only ingress routers are involved in the admission process.

As to aggregate reservations, these are envisaged using various types of tunnels. The term *tunnel* is used by QBone for an inter-domain reservation where one or both ends of the reservation are not fully specified (i.e., does not have fully specified IP address). The request to establish a tunnel may be administratively triggered or could be triggered based on historical data. [QBONEa] proposes separate procedures to establish a tunnel and to admit a flow that uses a tunnel.

The relationship between the presented bandwidth brokage and the IETF policy framework has not been addressed yet, but it is identified by the QBone project as a research topic. It is noted that IPHWY Inc. [IPHWY01], which offers a rudimentary bandwidth brokerage, has implemented proprietary extensions to the IETF model to incorporate the broker functionality.

The QBone group is currently considering a security architecture for their network.

Finally, it is noted that although the research and experimental work on the QBone architecture is still in early stages, it is progressing well. The current list of activities in this area can be found in [QBONEb].

3.4 Proposed M-NC&M framework

The proposed M-NC&M framework is shown in Fig. 9. The framework uses the concepts from IETF policy framework and the Internet2 bandwidth brokerage, described in the previous section. The main components of the M-NC&M are:

a. *Policy Administration* - responsible for consistent DiffServ offerings across all Defence Core domains. It controls multiple BB/PDPs, automatically distributes changes to the policy, and correlates feedback regarding about the health of the entire network;

b. *Bandwidth Brokers/Policy Decision Point* (BB/PDP) – plays a dual role, firstly acting as a PDP in relation to Policy Administration, and secondly performing typical Bandwidth Broker functionality;

c. *Other Policy Servers* – examples of such servers (not depicted in Fig. 9) include an authentication server and an accounting server;

d. *Policy Enforcement Points* – these are mainly DiffServ-enabled routers capable of enforcing QoS policy rules.

It is noted that Fig. 9 does not show any possible connectivity between BB/PDPs and other network management entities.

Below, components (a, b) are discussed in more detail.

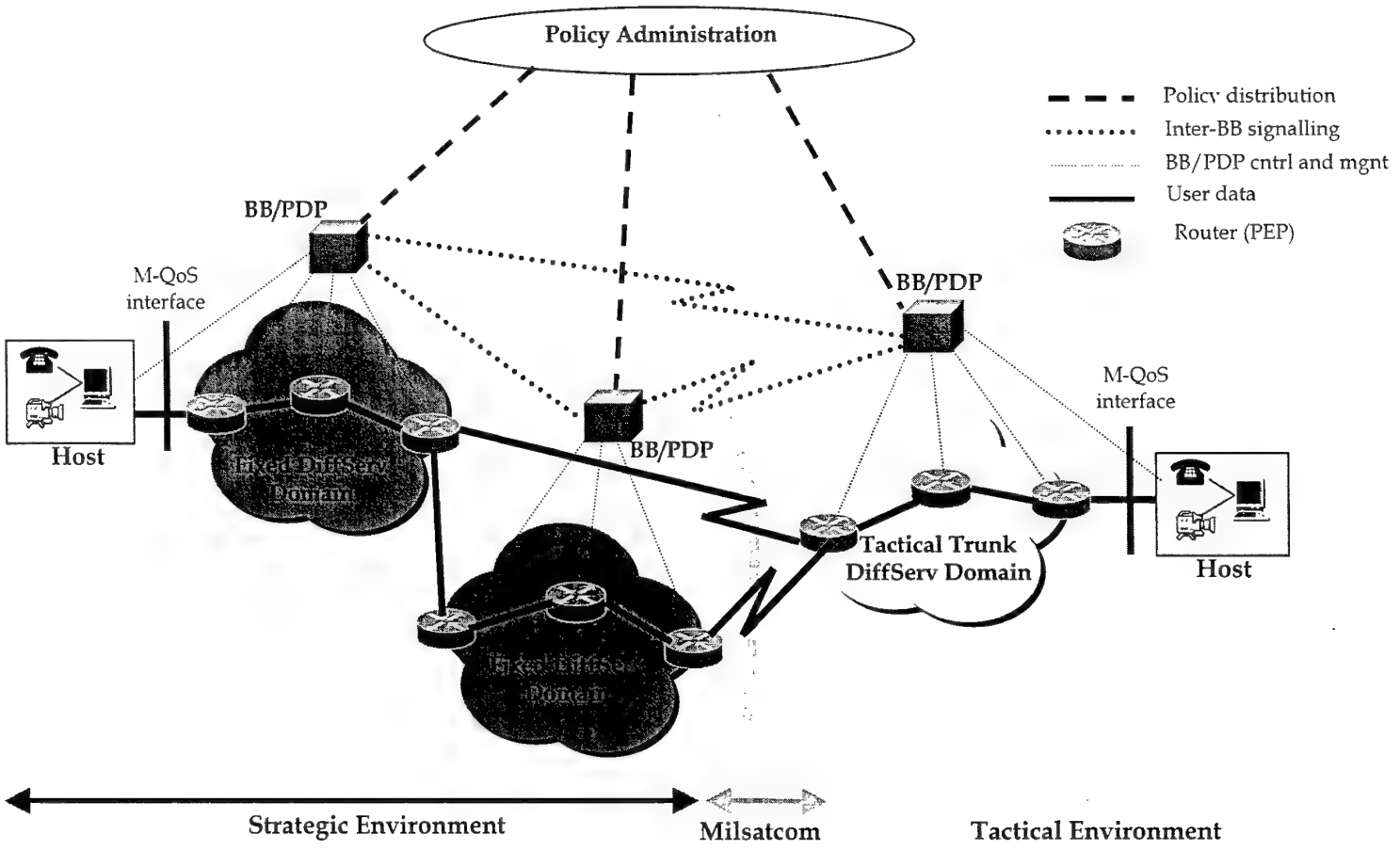


Fig. 9. Proposed M-QoS policy framework. NOTE: connections between BB/PDPs and other network management entities as well as other policy servers (e.g., authentication server) are not shown. (BB – bandwidth broker, PDP- Policy Decision Point, PEP- Policy Enforcement Point)

3.4.1 Policy Administration

To provide end-to-end M-QoS in the analysed part of Defence Core (see Section 1), policy administration needs to cover both (strategic) fixed and tactical trunk DiffServ domains. A complete centralisation of this administration in the strategic part of the Defence Core may not be desirable, mainly since the tactical trunk DiffServ domains are expected to have a substantial amount of policy information strictly related to their functioning in isolation. If only the strategic policy administration (PA) is to contain all this information, its distribution via low bandwidth/unreliable satellite links may potentially create performance/reliability problems.

Therefore, it seems to be beneficial to distribute policy management in the Defence Core. There are a number of possible approaches to this problem. A plausible one is presented in Fig.10 where a single PA controls all fixed DiffServ domains and each tactical trunk DiffServ domain has its own PA responsible for M-QoS delivery within the domain. To achieve consistent M-QoS across both types of domains, all policies have to be coordinated through some form of communication between the PAs (see Fig. 10) across satellite links.

3.4.2 Bandwidth Broker/Policy Decision Point

Our approach to bandwidth brokerage assumes that each DiffServ domain in the Defence Core will be equipped with a single BB/PDP entity performing both network control and management functions. The BB/PDP *control functions* will cover the following:

a. *Communication with end-user applications* using the concept of M-QoS interface described in [BLAC00], and briefly presented in Appendix A[11];

b. *Flow admission control*, which includes:

   - Authentication and authorisation of flow requests originating from end-user-applications;
   - Evaluation, according to the used network policy, of the Ultimate Priority[12] of military flows and their classification into one of the available classes;
   - Making decisions whether to admit flows into the domain and correspondingly reserving resources for them. The latter will be performed through configuration of ingress routers to impose classification and policing of the flows according to the negotiated Service Level Specifications (SLSs) and the current enterprise policy (obtained from policy administration);

[11] It is noted that MIN Branch, DSTO, is currently involved in software design for a standardised IP-based M-QoS interface between an end-user application and a BB.

[12] Appendix A briefly presents the way the Ultimate Priority of a flow can be evaluated.

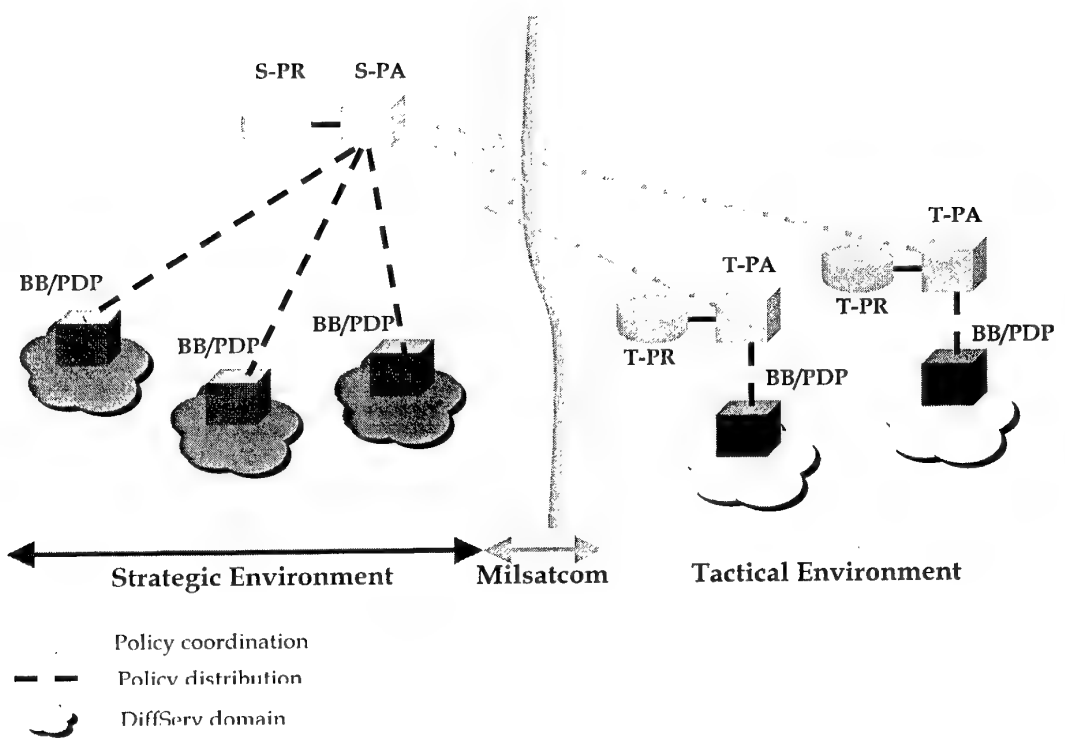


Fig. 10. An approach to the policy coordination/distribution in the analysed part of Defence Core. NOTE: Other policy servers (e.g., authentication server), not shown in this figure, may also be connected to BB/PDPs. (BB – bandwidth broker, PDP- Policy Decision Point, S-PA – strategic policy administrator, T-PA – tactical trunk policy administrator, S-PR – strategic policy repository, T-PR – tactical trunk policy repository).

- Evaluation of any time restrictions (i.e., timeliness) related to the (military) precedence level[13] of a flow. Such restrictions may trigger a change in the flow's classification at the ingress router (e.g., from flash level to routine level);

c. *Communication with end-user applications* using the concept of M-QoS interface described in [BLAC00], and briefly presented in Appendix A;

d. *Flow admission control*, which includes:

[13] Precedence, which refers to both timeliness and importance of a flow, is one of parameters specified by the end-user application when the flow set up is requested (see [BLAC00] for details).

- Authentication and authorisation of flow requests originating from end-user-applications;
- Evaluation, according to the used network policy, of the Ultimate Priority[14] of military flows and their classification into one of the available classes;
- Making decisions whether to admit flows into the domain and correspondingly reserving resources for them. The latter will be performed through configuration of ingress routers to impose classification and policing of the flows according to the negotiated Service Level Specifications (SLSs) and the current enterprise policy (obtained from policy administration);
- Evaluation of any time restrictions (i.e., timeliness) related to the (military) precedence level[15] of a flow. Such restrictions may trigger a change in the flow's classification at the ingress router (e.g., from flash level to routine level);

e. *Tracking SLSs of active flows in the domain;*

f. *Modification of resources reserved for pending flows.*

These modifications may be caused by:

- Admission of other, more important flows;
- Change of classification;
- Release of resources use by other flows;
- Fluctuations of the available bandwidth (e.g., due to errors in satellite links);
- A network failure which may lead to a traffic rerouting.

The modifications can be achieved by changing policing mechanisms (see Section 2.3.4) in ingress routers targeting particular flows, or through manipulating the minimum bandwidth allocated to PHBs in the class based queuing system (see Section 2.3.6);

g. *Releasing resource reservations* after the end-user application informs of the flow termination.

The following BB/PDP *management functions* are proposed:

a. *Communication with the policy administration.*

This communication includes receiving from the administration policy specifications and their updates, as well as sharing with the administration high-level information about intra- and inter-domain performance;

---

[14] Appendix A briefly presents the way the Ultimate Priority of a flow can be evaluated.

[15] Precedence, which refers to both timeliness and importance of a flow, is one of parameters specified by the end-user application when the flow set up is requested (see [BLAC00] for details).

b. *Retrieval of inter- and intra-domain routing information.*

This information will be stored in routers and/or other network management entities. It is expected that BB/PDPs will at least monitor the health of their own domains and connections with peer domains.

c. *Retrieval of performance statistics.*

These statistics regard the traffic exchanged inside the BB/PDP's own domain and with other peer domains, and based on these statistics, assessment as to whether the requested/promised QoS can be offered/maintained for flows initiated in the domain. If the QoS cannot be maintained, the BB/PDP may attempt to rectify the problem (e.g., reroute the traffic) or if the latter does not work, inform the end-user application about the inability to provide the promised QoS.

d. *Configuration of QoS-related parameters.*

A BB may configure resources (e.g., the minimum guaranteed bandwidth per PHB Group) in its all domain routers. This process will be performed according to the policy requirements obtained from the related policy administrator.

e. *Performing traffic engineering operations.*

Since traffic engineering may impact QoS, BB/PDPs are well suited to perform this function in relation to their DiffServ domains. MPLS mechanisms (see Section 2.4) can be used for this purpose. An approach to traffic engineering with the use of MPLS and bandwidth brokers in a DiffServ environment is presented in [RABB00].

f. *Deployment of inter-domain tunnels.*

The use of tunnels[16] may be required to diminish the amount of signalling traffic between BBs as well as to offer long-term reservations for traffic flow aggregates in a fashion similar to the Virtual Private Network (VPN) concept. These tunnels should be seen as an additional form of reserving resources orthogonal to DiffServ traffic classes.

It is stressed that the BB/PDP is a logical rather than a physical entity. Some form of distribution of its functions may be desirable, particularly if computational performance becomes an issue. A possible approach to BB distribution is described in [STEL00].

The QBone bandwidth broker architecture presented in Section 3.3 seems to be generic enough to implement the above control/management functions. However, a thorough investigation is required to assess the applicability of this architecture to the analysed part of Defence Core. In addition, it is stressed that although we use results from the QBone project, we do not preclude the use of concepts developed for other bandwidth broker architectures such as the ones mentioned in Section 3.1.

[16] The term tunnel is the same as used by QBone, and defined in Section 3.3.

3.5 Final remarks

We have shown that Policy-based Network Management and bandwidth brokerage can potentially support implementation of M-QoS in the Defence terrestrial/satellite Core.

The following Defence specific aspects of policy administration require further thorough investigation:

- Distribution of policy administration for the dispersed Defence fixed/tactical trunk communications involving (relatively) low bandwidth satellite links. Particular emphasis should be put upon performance and reliability issues;
- Specification of high-level M-QoS policies (see Fig. 5) in the Defence environment;
- Security aspects of policy administration.

There are a number of Defence specific unresolved issues related to the bandwidth brokerage functioning, including:

- *Specification of the detailed BB architecture including a definition of a viable flow admission control algorithm(s) that would satisfy the M-QoS concept, feedback to applications and performance monitoring; Performance aspects of BB-to-BB communication over (slow) satellite links.* This problem is out-of-scope of the Qbone project, and, to the best knowledge of the author, of any other civil research activities;
- *Impact of the security architecture on the use of bandwidth brokerage.* This issue relates to the impact of expected use of various forms of IPsec, including desktop-to-desktop, as well as the impact of partitioning Defence users to a number of intranet VPNs (e.g., SECBRS, BRS).

4. Conclusion and Recommendation

The major findings of this report can be summarised as follows:

a. The report argues that Military oriented QoS (M-QoS) can likely be implemented in a scalable and flexible way within the Defence terrestrial/satellite Core using a set of transmission technologies identified in a previous report (i.e., IPv4/IPv6, Differentiated Services (DiffServ), MPLS and ATM) in conjunction with bandwidth brokerage and Policy-based Network Management;

b. DiffServ is a crucial technology in providing scalable hard/soft QoS, prioritisation of IP flow aggregates, as well as graceful degradation in hard QoS of flows – the vital features of M-QoS;

c. Cisco routers are well equipped to implement DiffServ supporting the M-QoS features;

d. In the area of transmission technologies, the most challenging Defence-specific issues requiring further study are:

   - Mappings between DiffServ, MPLS and ATM technologies to implement M-QoS;
   - Traffic engineering using MPLS to support M-QoS.

e. The IETF's policy framework can be useful when implementing M-QoS oriented network management;

f. In the area of Policy-based Network Management, the most challenging Defence-specific issues are:

   - Distribution of policy administration for the dispersed Defence fixed/tactical trunk communications involving low bandwidth satellite links;
   - Specification of high-level M-QoS policies;
   - Security aspects of policy administration.

g. The Internet2's QBone bandwidth broker (BB) architecture seems to be generic enough to implement desirable control/management functions supporting M-QoS. However, the concepts developed for other bandwidth broker architectures should also be considered.

h. In the area of bandwidth brokerage, the most important Defence-specific problems are:

   - Specification of a detailed BB architecture;
   - Design of a viable flow admission control algorithm(s) that would satisfy the concept of M-QoS;
   - Performance aspects of BB-to-BB communication over satellite links.

- Use of bandwidth brokerage in the Defence secure environment.

Based on the report's findings, the following is recommended:

A. Continue to monitor the progress within:
   - The IETF policy-enabled network management architecture and its commercial developments;
   - The Internet2's QBone and other bandwidth broker management architectures and their commercial developments.

B. Undertake in the near term the following studies:
   - Analysis of the role of policies in future Defence network management;
   - Specification of high-level network management policy examples for Defence;
   - Specification of the detailed BB architecture including a design of viable flow admission control algorithm(s) and performance monitoring;
   - Analysis of inter-domain brokerage including performance issues pertaining to satellite bearers.

5. References

[ASHW01] P. Ashwood-Smith et al, "Generalized MPLS - Signaling Functional Description", IETF draft-ietf-mpls-generalized-signaling-04.txt, May 2001.

[BLAC00] P. Blackmore, P. George, M. Kwiatkowski "A Quality of Service Interface for Military Applications", Proceedings of MILCOM 2000 conference, Los Angeles, Oct 2000.

http://web-cd.dsto.defence.au/projects/core_comms/documents/papers/management/milcom00_final.doc

[BLAC01] P. Blackmore, P. George, K. Hui, P. Kerr, M. Kwiatkowski, K. Northeast, M. Rossiter, R. Taylor, C. Tran, "Review of the Defence Core Communications Environment", DSTO General Document, DSTO-GD-0275, Feb. 2001.

[BLAK98] S. Blake et al, "An Architecture for Differentiated Services", IETF RFC 2475, Dec. 1998.

[CHAN01] K. Chan et al, "COPS Usage for Policy Provisioning (COPS-PR)", IETF, RFC 3084, March 2001.

[CISC00] "Congestion Management Overview", Cisco Documentation, Aug. 2000.

http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/qos_c/qcprt2/qcdconghtm#xtocid84007

[CISC00a] "Cisco IOS Software and Multiprotocol Label Switching", Cisco, 2000.

http://www.cisco.com/warp/public/cc/pd/iosw/ioft/iofwft/prodlit/iosmp_ai.pdf

[CISC01] Cisco, "DiffServ – The Scalable End-to-End QoS Model", White Paper, 2001.

[DIFF01] Differentiated Services Charter, IETF.

http://www.ietf.org/html.charters/diffserv-charter.html

[DURH01] D. Durham et al, "The COPS (Common Open Policy Service) Protocol", IETF, RFC 2748, Jan. 2000.

[GARA00] A. Roy, "GARA: An Architecture for QoS", Proceedings of the First Joint Internet2 / DOE QoS Workshop: "QBone: Early Experiences and the Road Ahead", Houston, Feb. 2000.

[GEOR01] P. George, et al, "Implementation of the standardised Military oriented Quality of Service Interface for IP-oriented Networks", DSTO Technical Report, *in preparation*.

[GROS01] D. Grossman, "New terminology for Diffserv", IETF, draft-ietf-diffserv-new-terms-04.txt, March 2001.

http://www.ietf.org/internet-drafts/draft-ietf-diffserv-new-terms-04.txt

[HERZ00] S. Herzog et al, "COPS usage for RSVP", IETF, RFC 2749, Jan. 2000.

[INT201] Internet2, http://www.internet2.edu/

[IPHWY01] IPHIGHWAY Inc., " Policy Standards and IETF Terminology", White Paper, Jan. 2001.

http://www.iphighway.com/res-whitepapers.htm

[JACO99] V. Jacobson et al, "An Expedited Forwarding PHB", IETF RFC 2958, June 1999.

[KWIA99a] M. Kwiatkowski, P. George, "A Network Control and Management Framework Supporting Military Quality of Service", MILCOM'99, Atlantic City, USA, October 1999.

http://web-cd/projects/core_comms/documents/papers/management/milcom99_publ.doc

[KWIA99b] M. Kwiatkowski, "Network Control and Management Architectural Framework Supporting Military Quality of Service", DSTO Technical Report, DSTO-TR-0871, Sept. 1999.

http://203.10.217.101/corporate/reports/DSTO-TR-0871.pdf

[KWIA01] M. Kwiatkowski, "Preliminary Analysis of Transmission Technologies Supporting Military Oriented Quality of Service", DSTO Technical Report, *in preparation*.

[MOOR01a] B. Moore et al, "Policy Core Information Model -- Version 1 Specification", RFC 3060, IETF, Feb. 2001.

[MOOR01b] B. Moore et al, "Information Model for Describing Network Device QoS Datapath Mechanisms", draft-ietf-policy-qos-device-info-model-04.txt, IETF, June 2001.

[M60] "Recommendation M.60 – Maintenance Terminology and Definitions", ITU-T, March 1993.

[NORT00] Nortel Networks, "Passport 15000 Multiservice Switch", Product Brief, 2000.

http://www.nortelnetworks.com/products/library/collateral/80015.02-11-00.pdf

[NICH98] K. Nichols et al, "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers", IETF RFC 2474, Dec. 1998.

[POLI] IETF, Policy Charter, http://www.ietf.org/html.charters/policy-charter.html

[QBONE] QBone initiative, http://qbone.internet2.edu/

[QBONEa] QBone Bandwidth Broker Architecture (Work in Progress), June 2000.

http://qbone.internet2.edu/bb/bboutline2.html

[QBONEb] QBone Signaling Design Team

http://qbone.internet2.edu/bb/index.shtml

[QOSF99] QoS Forum, "The Need for QoS", White Paper, July 1999.
http://www.qosforum.com/tech_resources.htm

[RABB00] R. Rabbat et al, "Traffic Engineering - Using MPLS for Service Differentiation", Proceedings of the IEEE International Conference on Communications (ICC), 2000.

[RAP01] Resource Allocation Protocol Charter, IETF.
http://www.ietf.org/html.charters/rap-charter.html

[SHEN97] S. Shenker, C Partrige, R. Guerin, "Specification of Guaranteed Quality of Service", IETF RFC 2212, Sept. 1997.

[SNIR01] Snir Y, Ramberg Y, Strassner J, Cohen R, "Policy Framework QoS Information Model", draft-ietf-policy-qos-info-model-03.txt, April 2001.

[STAR99] QoS Forum, "Introduction to QoS Policies - White Paper", July 1999.
http://www.qosforum.com/white-papers/

[STEL00] R. Stelzl, "The Siemens Bandwidth Broker ", Proceedings of the First Joint Internet2 / DOE QoS Workshop: "QBone: Early Experiences and the Road Ahead", Houston, Feb. 2000.

[TEIT99a] B. Teitelbaum *et al*, "Internet2 Qbone: Building a Testbed for Differentiated Services", IEEE Communications Magazine, Sept./Oct. 1999.

[TEIT99b] B. Teitelbaum *et al*, "QBone Architecture (v1.0) ", Internet2, QoS Working Group, August 1999.
http://www.internet2.edu/qos/wg/papers/qbArch/1.0/draft-i2-qbone-arch-1.0.html

[WAHL97] M. Wahl et al, "Lightweight Directory Access Protocol (v3)", IETF, RFC 2251, Dec. 1997.

Appendix A: M-QoS Concept

Following the ITU rec. M60 [M60], Quality of Service (QoS) is understood in this report as the collective effect of service performances, which determine the degree of satisfaction of a user of the service. Performance measures include amount of bandwidth, transmission delay, jitter and error rate. Note that QoS is an end-to-end issue that relates to all networks involved in transmitting user information.

Generally, two basic types of QoS can be provided [QOSF99]:

- *Hard QoS* – the network offers an absolute reservation of resources for specific traffic; hard QoS is particularly important when a real-time flow[17] is to be transmitted, such as streamed video or audio;
- *Soft QoS* – some traffic is offered a statistical preference (e.g., faster packet handling, lower probability of packet discards) over the rest.

In commercial networks, if not enough free network resources are available to establish/maintain a flow with the required hard QoS, a typical approach is to release the flow, and offer no graceful degradation in QoS.

However, as argued in [KWIA99a], in military packet networks, when not enough network resources are available to support hard QoS for all traffic flows, the flows carrying mission critical information should get preference (i.e., higher priority) over less important flows. In addition, in overloaded networks, it is preferable to gracefully "step down" the hard QoS of less important military flows instead of automatically tearing down these flows. The end-user application, rather than the network, should decide whether the offered hard QoS is sufficient to continue the flow. On the other hand, the network, not the end-user application, decides whether and which flows should gracefully degrade. Finally, higher flow priorities should be given for a restricted time defined by the doctrine.

The commercial QoS in conjunction with the above listed features are jointly called Military oriented QoS (M-QoS).

It is noted that as in the case of the commercial QoS, M-QoS is also an end-to-end issue. Note also that the proposed M-QoS concept does not refer to all flows that could potentially traverse a military network, but only to those, which carry military essential information and require hard/soft QoS.

To provide M-QoS, it is crucial to design a standard interface, called the *M-QoS interface*, between an end-user application and network control and management. A framework for such an interface within the context of policy-enabled networks is proposed in [BLAC00] and used in this report. The interface is generic in the sense that it assumes a set of military specific parameters are used to evaluate the ultimate

[17] Following [SHEN97], a flow is understood in this report as a set of packets traversing a network, all of which are covered by the same request for control of QoS.

priority of the flow according to policy(ies) currently implemented on the network. The interface enables:

1. The end-user application to specify commercial QoS specific parameters (e.g., maximum bit rate, maximum packet/cell delay) which determine the amount of network resources to be reserved to satisfy the required QoS;
2. The end-user application to define (qualitative) military specific parameters, including *Mission Identification*, *Precedence* (which refers to both timeliness and importance of a flow) and *User Perceived Priority;*
3. The network control and management to inform the application about problems in delivering the requested/promised QoS.

Parameters described in (1,2) are used by the network control and management to evaluate the *Ultimate Priority* of the flow according the algorithm described by the enterprise policy.

Robust software for the interfacewhen used in Defence IP-oriented environment has been developed by DSTO and presented in [GEOR01]. This software can be a part of the end-user application and then it can perform all functions (1-3) above. It can also be used an adjunct, which interfaces with network control and management on the application's behalf. In this case, the application only sends and receives data from the transmission network.

DISTRIBUTION LIST

Report title
A Concept of Defence Core Communication Infrastructure Supporting M-QoS

Author
Marek Kwiatkowski

AUSTRALIA

DEFENCE ORGANISATION

Task sponsor

Director General Command, Control, Communications and Computers (DGC4)
Mr. Claude D'Abrera (DDFC), R1-3-A079A
CMDR Paddy Torrens (DD-MOBILE COMMUNICATIONS), R1-3-A067
WGCDR Eric Gidley (DDLRC), R1-3-A103

S&T Program

Chief Defence Scientist
FAS Science Policy
AS Science Corporate Management
Director General Science Policy Development
} shared copy

Counsellor Defence Science, London (Doc Data Sheet only)
Counsellor Defence Science, Washington (Doc Data Sheet only)
Scientific Advisor to MRDC Thailand (Doc Data Sheet only)
Scientific Advisor Joint
Navy Scientific Adviser (Doc Data Sheet and distribution list only)
Scientific Adviser - Army (Doc Data Sheet and distribution list only)
Air Force Scientific Adviser
Director Trials

Aeronautical and Maritime Research Laboratory
Director

Electronics and Surveillance Research Laboratory
Director (Doc Data Sheet and distribution list only)

Chief of Communications Division
Research Leader Military Information Networks
Head Network Architectures
Head Wireless Systems
Head Network Management
Head Distributed Systems Group (Fern Hill)
Marek Kwiatkowski (DSTO/CD/MIN)

DSTO Library and Archives
Library Fishermens Bend (Doc Data sheet only)
Library Maribyrnong (Doc Data sheet only)
Library Salisbury (1 copy)
Australian Archives
Library, MOD, Pyrmont (Doc Data sheet only)

US Defense Technical Information Center, 2 copies
UK Defence Research Information Centre, 2 copies
Canada Defence Scientific Information Service, 1 copy
NZ Defence Information Centre, 1copy
National Library of Australia, 1 copy

Capability Development Division
Director General Maritime Development (Doc Data Sheet only)
Director General Land Development (Doc Data Sheet only)
Director General Aerospace Development (Doc Data Sheet only)

Defence Materiel Organisation
DCNSPO, R3 Russell Offices, Canberra

Knowledge Staff
Director General Intelligence, Surveillance, Reconnaissance, and Electronic Warfare (DGISREW) R1-3-A142, Canberra, ACT 2600
Director General Defence Knowledge Improvement Team (DGDKNIT) R1-3-A141, Canberra, ACT 2600 (Doc Data Sheet only)

Navy
SO (Science), Director of Naval Warfare, Maritime Headquarters Annex, Garden Island, NSW 2000 (Doc Data Sheet only)
Directorate of Navy Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance and Electronic Warfare, CP4-4-043

Army
ABCA Standardisation Officer, Puckapunyal (4 copies)
SO (Science), DJFHQ(L), MILPO Enoggera, Queensland 4051 (Doc Data Sheet only)
NAPOC QWG Engineer NBCD c/-DENGRS-A, HQ Engineer Centre Liverpool Military Area, NSW 2174 (Doc Data Sheet only)

Intelligence Program
DGSTA Defence Intelligence Organisation
Head, Information Centre Defence Intelligence Organisation

Information Systems Division
HISD, CP1-5-001, Department of Defence, Canberra ACT 2600
DGIS-ISD, DKN-N1-007
DDC-ISD, DKN-N1-005
Mr. Ric Glenister, DKN-N1-30
Mr. Bert Hunter, DKN-N2-A11-A13

Corporate Support Program
Library Manager, DLS Canberra

Universities and Colleges
Australian Defence Force Academy
Library
Serials Sections (M list), Deakin University Library, Geelong, 3217
Senior Librarian, Hargrave Library, Monash University (Doc Data Sheet only)
Librarian, Flinders University

Other Organisations
NASA (Canberra)
AusInfo
State Library of South Australia

OUTSIDE AUSTRALIA

Abstracting and Information Organisations
Engineering Societies Library, US
Documents Librarian, The Center for Research Libraries, US

Information Exchange Agreement Partners
Acquisitions Unit, Science Reference and Information Service, UK
Library – Exchange Desk, National Institute of Standards and Technology, US

SPARES (5 copies)

Total number of copies: 56

DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION
DOCUMENT CONTROL DATA

1. PRIVACY MARKING/CAVEAT (OF DOCUMENT)

2. TITLE

A Concept of Defence Core Communication Infrastructure Supporting M-QoS

3. SECURITY CLASSIFICATION (FOR UNCLASSIFIED REPORTS THAT ARE LIMITED RELEASE USE (L) NEXT TO DOCUMENT CLASSIFICATION)

Document	(U)
Title	(U)
Abstract	(U)

4. AUTHOR(S)

Marek Kwiatkowski

5. CORPORATE AUTHOR

Electronics and Surveillance Research Laboratory
PO Box 1500
Edinburgh, SA 5108 Australia

6a. DSTO NUMBER	6b. AR NUMBER	6c. TYPE OF REPORT	7. DOCUMENT DATE
DSTO-TR-1220	AR-012-032	Technical Report	October 2001

8. FILE NUMBER	9. TASK NUMBER	10. TASK SPONSOR	11. NO. OF PAGES	12. NO. OF REFERENCES
E 8709-7-16-2	99/150	C4	51	112

13. URL
http://www.dsto.defence.gov.au/corporate/reports/DSTO-TR-1220.pdf

14. RELEASE AUTHORITY

Chief, Communications Division

15. SECONDARY RELEASE STATEMENT OF THIS DOCUMENT

Approved for Public Release

16. DELIBERATE ANNOUNCEMENT

No Limitations

17. CASUAL ANNOUNCEMENT Yes

18. DEFTEST DESCRIPTORS

Network Control, Network Management, Computer Architecture, Switching Systems, Quality of Service, Military Networks

19. ABSTRACT

This report is a continuation of DSTO's research effort in the area of Military oriented Quality of Service (M-QoS) and presents an architectural concept of network transmission, control and management that would offer M-QoS features over the Defence terrestrial/satellite Core environment communications infrastructure. The report first discusses in more detail the use of the transmission framework proposed in an earlier study by the same author, with particular emphasis put upon IP Differentiated Services - a vital technology to implement M-QoS. Then, a Military oriented Network Control and Management (M-NC&M) framework, based on policy-enabled networking and bandwidth brokerage that would facilitate the implementation of M-QoS is described. The M-NC&M framework utilises results from the IETF's standardisation effort on policy framework and work from the Internet2 on bandwidth brokerage. Finally, a number of future research studies supporting the architectural concept are proposed in the report.

TECHNICAL REPORT DSTO-TR-1220 AR-012-032 OCTOBER 2001

DEPARTMENT OF DEFENCE
DEFENCE SCIENCE & TECHNOLOGY ORGANISATION
DSTO

ELECTRONICS AND SURVEILLANCE RESEARCH LABORATORY
PO BOX 1500 EDINBURGH SOUTH AUSTRALIA, 5111
AUSTRALIA, TELEPHONE (08) 8259 5555